Försättsblad tentamen/ Examination cover

10597696

Anonymkod / Anonymous code

0	0	1	3	-	C	B	M

Skriv anonymkod på varje ark / Write anonymous code on all sheets

D	T	5	2	3	A

Datasäkerhet

A	0	0	1

Teori

2	0	2	3	-	0	5	-	2	9

Tentamensdatum / Exam date

Ifylles av tentamensvakt / To be filled by the invigilator

Antal inlämnade ark: 09

Signatur: _____

Resultat / Results

Ifylles av lärare / To be filled in by teacher

1	2	3	4	5	6	7	8	9	10
1	-0,25	1	1	1	1	1	1	1	1

11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1

Totalpoäng
25,25

6,5 + 18,75 =

Betyg / Grade					
F	E	D	C	B	A
☐	☐	☐	☒	☐	☐

0	0	1	3	-	C	B	M

Utskriven 2023-05-23 kl. 09:32:56

ÖREBRO UNIVERSITET

L

Anonymkod / Anonymisation code:
0013-CBM

Sidnr / Page no: 1

Uppgift nr / Question no: 'Open question'

Poäng / Score: 1,5+2+1,5+0+1+1

Lärarens anteckning / Teacher's notes:

Definitions:

Passive attacks' main purpose is to gain knowledge about an IT system, without "making a mark", meaning no modifications, disruptions or the like, of the system. ✓

Active attacks aim to alter / modify an IT system, or deny service for regular users. ✓

Examples:

Passive:

(1) Eavesdropping on a wireless network.
(2) Packet sniffing and traffic analysis going through some router.. ✓

I WOULD ARGUE THAT SNIFFING IS A TYPE OF EAVESDROPPING

Active:

(1) SQLi, to modify IT systems' databases. Example: increase 'likes' on a social media post. ✓
(2) DDOS using a BotNet, denying service to the IT system for regular users.

IN GENERAL, YOU COULD HAVE EXPANDED YOUR ANSWERS

Örebro universitet

Skriv ej på baksidan. – Do not write on the back of the sheet.

ÖREBRO UNIVERSITET

L

Anonymkod / Anonymisation code:
0013-CBM

Sidnr:
Page no:
2

Uppgift nr:
Question no:
Single Choice questions

Poäng:
Score:

Lärarens antecknig:
Teacher's notes:

1	D
2	C
3	A
4	A
5	C
6	C
7	A
8	B
9	B
10	A
11	D
12	A
13	A
14	B
15	D
16	C
17	A
18	C
19	A
20	B

(Answers also written, redundantly, on the question papers too!?)

Örebro universitet

Single Choice Questions (20 points in total)

Q1 - A malware infection can be a threat for D.

[A] Integrity

[B] Availability

[C] Confidentiality

[D] All of the above answers

Q2 - Digital signatures and key management are important components of C cryptography.

[A] Private-key

[B] Public-key

[C] Advanced

[D] Symmetric

Q3 - The A sends messages on a regular basis to verify that the device is still operational and to provide feedback about the internal status of the device.

[A] Heartbeat protocol

[B] HTTP protocol

[C] Alert protocol

[D] Handshake protocol

Q4 - To provide assurance that a delivered message is correct (as sent by the sender), it is possible to append to the message the A.

[A] Message Authentication Code (MAC)

[B] **Media Access Control (MAC)**

[C] Electronic Codebook (ECB)

[D] Block Cipher

Q5 - Recognition by fingerprint, retina, and face are examples of C.

[A] Face recognition

[B] Dynamic biometrics

[C] Static biometrics

[D] Token authentication

Q6 - Which one of these vulnerabilities is NOT a vulnerability of password-based authentication?

[A] Dictionary attacks

[B] Brute-force attacks

[C] Non-revocability

[D] Workstation hijacking

Q7 - S/MIME is a protocol used for A .

(A) Sending digitally signed and encrypted messages

[B] Hiding information in images through steganography

[C] Mimicking messages and delivering Man-in-the-Middle (MitM) attacks

[D] Establishing a secure SSL connection between two devices

Q8 - B is a technique used by an attacker to collect infected users' clicks, usually using a transparent window, leading the users to think that they pressed the intended buttons or typed in the correct forms.

[A] Social engineering

(B) Clickjacking

[C] Ransomware

[D] Keylogging

Q9 - The B contains the set of events or conditions that determines when the payload of a virus is activated or delivered.

[A] Infection mechanism

(B) Logic bomb

[C] Payload

[D] Dormant phase

Q10 - The replay attack is a network attack that consists in A.

[A] Intercepting a data packet and retransmit it later to the victim

[B] Creating a data packet and transmitting it many times to overwhelm a victim

[C] Sending repeatedly the same packets in different order, to disorient the victim

[D] Opening multiple network connections, without completing any handshake

---

Q11 - The main disadvantage of encrypting a database, or parts of it, is that D.

[A] It is really expensive

[B] Can increase the chances of losing valuable data

[C] DB access control does not work anymore

[D] It is more difficult to perform record searching

Q12 - A use the same communication channel for injecting SQL code and retrieving results.

[A] In-band attacks

[B] Inferential attacks

[C] Out-of-band attacks

[D] Side-channel attacks

Q13 - A A monitors the characteristics of a single host and every event occurring within that host for suspicious activity.

[A] Host-based IDS

[B] Firewall

[C] Network-based IDS

[D] Anti-virus

Q14 - B collects the behaviour of users on systems or networks, and analyses the data points to identify if there is any deviation from the expected data, signalling a potential intruder.

[A] Profile-based detection

[B] Anomaly detection

[C] Threshold detection

[D] Signature/heuristic detection

Q15 - A consequence of a buffer overflow error is D.

[A] Corruption of data used by a program

[B] Unexpected transfer of control in a program

[C] Possible memory access violation

[D] [All the previous answers are true]

Q16 - Firewalls aim to filter C.

[A] Only outgoing traffic

[B] Only ingoing traffic

[C] Both ingoing and outgoing traffic

[D] Incoming malwares

Q17 - A is an automated technique that involves providing invalid, unexpected, or random data as inputs to a system to verify its robustness.

[A] Fuzzing testing

[B] Unit testing

[C] GUI testing

[D] Functional testing

Q18 - Defensive programming is C.

[A] A technique for configuring correctly a firewall installed in a network

[B] The process of producing software for defending a computer and/or a network

[C] A software design approach for producing software that continues to function under attack

[D] None of the above

Q19 - A is the right to exclude others from making, using, offering for sale, or selling an invention.

[A] Patent

[B] Trademark

[C] DRM

[D] DMCA

Q20- To compensate for ambiguities that could arise from uncertain laws, many professionals and societies adopted B.

[A] Access control policies

[B] Codes of conduct

[C] Digital Rights Management (DRM)

[D] Privacy protection